Migrating servers, elusive users: reconfigurations of the Russian Internet in the post-Sowden era

Ermoshina, Ksenia; Musiani, Francesca

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: reconfigurations of the Russian Internet in the post-Sowden era. *Media and Communication*, *5*(1), 42-53. https://doi.org/10.17645/mac.v5i1.816

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 42–53
DOI: 10.17645/mac.v5i1.816

Article

Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era

Ksenia Ermoshina and Francesca Musiani *

Institute for Communication Sciences, 75013 Paris, France; E-Mails: ksenia.ermoshina@cnrs.fr (K.E.), francesca.musiani@cnrs.fr (F.M.)

* Corresponding author

Submitted: 4 November 2016 | Accepted: 23 January 2017 | Published: 22 March 2017

Abstract
In response to the growing censorship of their national Internet, Russian users, content producers and service providers have developed several resistance tactics. This paper analyzes these tactics with particular attention paid to their materiality. It first addresses the different levels of Internet "governance by infrastructure" in Russia, then focuses on the different tactics of individual and collective resistance and concludes by discussing how forms of control enacted at different levels of infrastructure are reconfiguring the geopolitics of the Russian Internet.

Keywords
digital sovereignty; Edward Snowden; Internet geopolitics; Internet governance; Internet infrastructure; resistance; Russian Internet

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

The last two decades of Russian Internet (RuNet)'s development have showed a paradoxical situation where a rapidly developing[1] Internet coexisted with a state-centered Internet governance. A "half-freedom of speech" (Gelman, 2010) was associated with the hope of a democratization of the country (Elting et al., 2010; Lonkila, 2012). However, after the defeat of the protest movement "For Fair Elections" (2011–2012), these democratic expectations were questioned. The Kremlin started seeing the Internet "as politically disruptive because it enables citizens to circumvent government-controlled 'traditional' media" (Nocetti, 2015, p. 113).

Recent developments in RuNet regulation demonstrate the government's will to establish national control of the digital sphere (Freiberg, 2014; Nocetti, 2015). The presidential administration organized an "Internet + Sovereignty" forum in May 2016 around issues of national governance of the Internet of Things (IoT) and Big Data, promoting a project of Russian standards and the possibility of building a closed national network in the field of IoT. The intention to develop a "sovereign Internet" was also proposed as a double response to the terrorist threat and the domination of American web services.

However, the laws that frame online activities of Russian users are diverse and constantly evolving as a patchwork of incomplete measures that overlap and sometimes contradict each other. Each of these measures challenges IT professionals, e.g. Internet service providers, hosting providers, developers, journalists, bloggers and NGOs. Simultaneously, a set of individual practices, know-how, or *arts de faire*, is being developed by RuNet users to bypass access restrictions or protect their communications from governmental surveillance.

[1] 75% of population are said to have Internet access in 2016.

Emerging NGOs and associations promote and institutionalize some of these hacks and launch large-scale campaigns for RuNet freedom.

In light of this context, the central research aim of this paper is to understand the connection between the "State-centered" style of Russian Internet governance and the local tactics of *détournement* and bricolage (Akrich, 1998). Our hypothesis is that in the Russian case, resistance to Internet control and surveillance happens not only and not *primarily* at the political and legal levels (e.g. lobbying or negotiations with governmental structures, class action or collective mobilizations) but at the level of everyday individual practices of usage, such as anonymization of users or migration of people and infrastructures. A specific body of research dedicated to local social movements in contemporary Russia (Erpyleva & Magun, 2014; Kharkhordin, 2011; Prozorov, 2012; Zhuravlev, Savelyeva, & Yerpylova, 2014) is helpful to analyze this style of contention: indeed, this research analyzes post-Soviet de-politicization as the consequence of an "exodus" from the public sphere to the private sphere. It shows that Russian civil society tends to mobilize around local problems, often related to the materiality of the city (Ceruzzi, 2006) rather than to support global challenges; for example, bottom-up activities of repair and maintenance of a particular district or equipment in the city will be favored over a protest against the Mayor of the same city. In this sense, and along the lines of recent scholarship such as Klyueva's (2016), the article is also an attempt to understand the specificities of the response of Russian civil society—with its mix of collective and individual tactics of resistance—to restrictive Internet policies.

The structure of the paper is as follows. First, it addresses the different levels of Internet "governance by infrastructure" (DeNardis & Musiani, 2016), in Russia—showing how the Russian State is increasingly leveraging, co-opting and on occasion "tampering with", Internet infrastructure in order to fulfill political aims that, in some instances, are sensibly different than the objectives the infrastructure was originally meant for. Then, the paper focuses on the different tactics of individual and collective resistance, and concludes with a discussion of how the forms of control enacted at different levels of RuNet infrastructure are reconfiguring its geopolitics.

The paper builds upon observations of "cryptoparties", on original interviews with Russian IT-specialists, Internet service providers (ISPs) and expatriate journalists and developers, and situates this material by means of a brief analysis of Russian Internet legislation. More specifically, the empirical part of the research combined several methods: observation of three cryptoparties in 2012, 2015 and 2016—the purpose of these observations being to analyze different tools used in order to protect anonymity and bypass censorship, as well as the discourse organizers and participants were developing about Internet regulations in Russia; interviews with 3 internet service providers, 4 expatriated developers, 1 NGO organizer and a dozen users. The interviews were semi-structured with grids adapted to providers, developers and users, and lasted between 40 minutes and 2 hours. Qualitative analyses of relevant press materials and Web ethnographies analyzing professional forums of ISPs as well as the biggest Internet resources dedicated to Internet Freedom in Russia (such as Moskovskiy Libertarium or Rublacklist) were also conducted.

2. Surveillance, Data Storage and Filtering: Levels of Infrastructure-Based Internet Control in Russia

RuNet governance has developed upon several layers, with three main types of measures adopted since 1998:

a) Surveillance measures of 'lawful interception', called System of Operative Investigative Measures (SORM), aimed at giving governmental services such as FSB (former KGB) access to private communications both by telephone and on the Internet;[2]
b) Regulation of data storage, restricting important data flows to national borders;
c) Filtering measures, restricting access to a growing list of websites (blacklist)[3] considered as extremist. These three layers are interconnected and show a global tendency towards a RuNet "balkanization"—hyper-localization and nation-state regulation of data and communication flows.

2.1. "SORMisation" of Russia: Surveillance Measures and ISP Markets

The SORM was first implemented in Russia in 1998. SORM provides an architecture by which law enforcement and intelligence agencies can obtain direct access to data on commercial networks. During the past eight years, SORM has given rise to new configurations of sociotechnical "actants" (Latour, 1988) with long-term consequences on the market of ISPs. Three generations of SORM measures have seen the light. SORM-1 allows FSB to access telephone traffic, including mobile networks. SORM-2, implemented in 2005, is responsible for inter-

[2] Apart from FSB and Roskomnadzor, MVD (Ministry of Internal Affairs), FSO (Federal Service of Security), FSKN (Federal Service for Control of Drug Traffic), FTS (Federal Customs Service) and FSIN (Federal Penitentiary Service) also participate in online surveillance in Russia. However, while MVD, FSB and FSKN both possess the equipment and have the right to use it for lawful interception, FSO and FTS depend on FSB to have an access to the equipment, while FSIN has the equipment but does not have the right to use it for investigative activities. Apart from state actors regulating online surveillance, a market of surveillance equipment has been developing in recent years (especially since the adoption of SORM-3 measures). Several private companies seem to play the most important role in this field: "Special technologies" and "MFI-Soft" (who earn 5–6 billion rubles a year on SORM equipment) and smaller manufacturers (Reanet, Norsi-Trans and TechArgos each earning 1 billion rubles a year). The most recent player on the market is the State corporation RosTech, supposed to produce the necessary equipment to implement Yarovaya law.

[3] Officially called "Unified Register of Domain Names, Internet Website Page Locators, and Network Addresses that Allow to Identify Internet Websites Containing Information Prohibited for Distribution in the Russian Federation" (or Unified Register).

cepting IP traffic, including VoIP. SORM-3, implemented in 2014, gathers information from all communication media, and offers long-term and comprehensive storage of subscriber data (Privacy International, 2016).

Compared to international Lawful Interception standards, SORM gives great autonomy to surveillance actors. In most Western countries, law enforcement agencies seek a warrant from a court and then issue an order for lawful interception to a network operator or ISP, which is obliged to intercept and deliver the requested information. The FSB does not need to contact the ISP because of the very architecture of SORM, containing two main elements: the "extractor" (the equipment—software and hardware—that performs data extraction) and the "remote control station". The control station is localized in the FSB regional office and enables remote control of the extractor without the provider's permission: the provider may not know which data, and how, is intercepted, analyzed and transferred. No court decision is necessary in order to activate the interception of the metadata. However, in order to access the actual telephone recordings, FSB has to ask for a court permission. In 2012, there were 372,144 orders distributed, according to the official data provided by the Supreme Court.[4]

The most expensive component of SORM is the circular buffer for data storage. However, each new generation of SORM measures has changed the technical requirements: while for SORM-2 providers needed to store all the traffic for 12 hours, SORM-3 obliged them to store all the metadata for three years. Thus, the providers have to change all their equipment as the implementation of SORM systems completely relies on them: "We pay for it", remarks internet provider Michael I. "If you do not put this equipment, you do not have license and you lose state clients".

When the local FSB or prosecutor's office identifies shortcomings, they send the information to Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media).[5] The ISP is warned, first fined, then if violations persist, its license may be revoked (Borogan & Soldatov, 2013). Roskomnadzor statistics show that in 2010, there were 16 warnings, 13 in 2011, and 30 in 2012.[6]

Providers have to renew SORM equipment by themselves as no certified standards exist on the market and there is no consensus among manufacturers. As a result, providers have to adapt to the new technical demands, sometimes via DIY tinkering with old equipment: "Adapt the parts of your system, first of all…because when they will finally publish the certificates…we will have to spend tons of bucks again, and we will have to do it, because that's the Law",[7] notes user Andrei on 14 November 2015.

An inquiry led by Leonid Volkov, activist, blogger and programmer, claims that "a small provider has to give about 20%–30% of his annual income to buy SORM equipment" (Volkov, 2016). The two biggest manufacturers of SORM equipment earn 5–6 billion rubles per year on SORM, while three other small manufacturers earn about 1 billion. To reduce their costs, smaller providers buy SORM-as-a-service from their upstream providers. The implementation of SORM-1 in Russia sparked a protest campaign by IT-professionals, human rights organizations and Internet freedom defenders. The first anti-SORM movement was launched in the late 1990s in the form of a DDoS attack on FSB semantic analysis tools. Activists were adding specific keywords to every mail, such as "bomb", "explosion", "terrorist attack", triggering constant alerts to the control station and overloading it. Moscovskiy Libertarium,[8] with Russian and international partners, launched an international solidarity campaign against SORM. A public petition was sent to the Supreme Court and former Russian president Boris Yeltsin, asking him to "use his authority in order to stop the implementation of SORM", an "unprecedented example of violation of the rights to privacy and human rights convention".[9] While this campaign did not produce immediate results, fifteen years later the European Court of Human Rights has recognized that SORM was a violation to the European Convention of Human Rights, because its technical infrastructure enabled interception of communications without court permission, thus bypassing legal procedures.

The early-2000s anti-SORM campaign was mostly led by journalists, NGO activists and programmers, while providers were almost absent from the controversy, with the exception of "Bayard-Slaviya Communications". As Sergey Smirnov, activist of Pravozashitnaya Set (Human Rights Network), notes: "Internet service providers have come to the conclusion that the perspective to lose their license is much worse than the necessity to collaborate with FSB. In one of the recent publications about SORM, an FSB officer noticed that in the majority of cases providers apply all the requirements without any pressure and even demonstrate an understanding".[10] The

[4] According to the official statistics provided by the Supreme Court, in 2012, 372,144 orders were distributed, compared to 326,105 in 2011, 276,682 in 2010, 245,645 in 2009, 229,144 in 2008 and 189,591 in 2007: https://ria.ru/infografika/20130815/956535235.html

[5] Roskomnadzor is a Federal Executive Authority of the Russian Federation, performing the following functions: control and supervision of mass media (including electronic mass media), mass communications, information technology, and telecommunications; supervision and statutory compliance control of personal data processing; managing the Radio Frequency Service activities; supervision of production of copies of audiovisual works, computer software, databases and audio recordings on any media; accreditation of experts and expert organizations for content evaluation in order to ensure child information security. It is affiliated to the Ministry of Communications and Mass Media of the Russian Federation. The role of Roskomnadzor has recently expanded. The list of all its functions may be found on its official website: http://eng.rkn.gov.ru/about

[6] Available at https://rkn.gov.ru/press/annual_reports

[7] Available at http://forum.nag.ru/forum/index.php?showtopic=47641&st=560

[8] Available at http://www.libertarium.ru, created by Anatoliy Leventchuk in 1994.

[9] Available at http://www.libertarium.ru/l_sormact_gilc

[10] Available at http://www.libertarium.ru/l_sormact_conf6aprd

lack of providers in the anti-SORM movement made any civil disobedience movement technically impossible. In order to create a precedent, Leonid Volkov launched a campaign against SORM-3 in 2015; he started the so-called "Attack on SORM", a legal and political project of collective appeal to court by operators and providers, to demand better regulation of SORM and state-funded certified equipment.

2.1.1. Yarovaya Law: When Law (Unusually) Pre-Dates Technology

Nonetheless, the development of SORM legal and technical requirements created tensions in the ISP community. In June 2016, a new set of surveillance measures was proposed by Representative Irina Yarovaya: Russian telecom operators will have to store all traffic (including calls, letters, documents, images and video) for six months, and related metadata for three years. The importance of this case lies in its revealing a "reverse gap" between legal measures and financial and technical resources: while "governments are struggling to keep up with the pace of technological change, with technology evolving faster than law-making efforts" (Nocetti, 2015, p. 111), in the Yarovaya law case, law-making has outpaced the actual technological development of the country. Indeed, such surveillance needs a complex and multilayered technical infrastructure (including servers, the network itself, data storage systems and software), with far-reaching implications for the ways Internet and telecommunications work in Russia, including quality of connection, the speed at which and the amounts of data the network is able to transfer and the price of Internet services. Vladimir K., ISP, says: "Yarovaya law is technically absurd. Firstly, there is no necessary equipment on the market. Secondly, it is useless to store encrypted data. With the same success, we can code a random numbers generator and send this data to FSB pretending it is our users' traffic".

The problem is both technical and geopolitical, as it questions the limits of the Russian nation-state and its capabilities to implement a new infrastructure independently from the Western market. Within embargo, due to the Western sanctions imposed on Russia following the annexation of Crimea in 2014, the Russian government turns to national companies to produce the necessary equipment. The politics of "substitution of imports" coupled with the new series of surveillance laws have an important impact on the Russian IT-industry. The CEO of MGTS (Moscow State Telecom Network), Andrey Ershov, states: "Today we do not have any equipment in order to be able to put the 'Yarovaya law' into practice….So, the biggest concern that all telecom operators publicly express, is related to the cost of such solutions. [The equipment] is about tens of billion rubles". Even the emerging set of firms specialized in SORM equipment cannot satisfy Yarovaya law requirements in terms of equipment, estimated at 10.3 billion rubles (Kantyshev, 2016). Providers and telecom operators have publicly expressed their skepticism of the new surveillance law, pointing out that new solutions risk becoming obsolete within a few years and will demand further investment (Schepin, 2016). Press and specialized websites show a rise in disapproval of the Yarovaya law among IT professionals, for similar reasons. Among the actors criticizing the law are the biggest Russian IT companies, Mail.ru and Yandex, as well as professional associations Russian Association of Electronic Communications and Russian Civic Organization Center for Informational Technologies and even a pro-governmental working group "Communications and IT" ("Svyaz i IT"). The most popular professional forum of Russian providers, Nag.ru, creatively reacted to the law by developing a "Yarculator"[11], a software enabling providers to calculate the prices for the necessary equipment and the cost of Internet services for end users.

The law was largely contested by civil society. A petition on Change.org gathered 623,465 signatures as of 8 January 2017. A demonstration against the law was held in Moscow in August 2016 and gathered between 2,400 to 4,000 people (Kozlov & Filipenok, 2016). On his end, Edward Snowden publicly asked Putin not to sign the Yarovaya law, emphasizing its nefarious economic consequences and pointing out that a six-month storage of data is dangerous, unfeasible and expensive[12] (Figures 1 and 2).

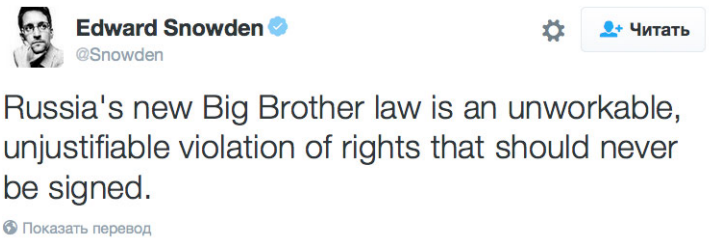

Figure 1. Edward Snowden's critical tweet on the Yarovaya law.

[11] Available at http://nag.ru/articles/article/29513/-yarkulyator-kalkulyator-yarovoy.html#comments
[12] Available at http://www.macdigger.ru/iphone-ipod/snouden-raskritikoval-zakon-yarovoj-on-otnimet-u-rossiyan-dengi-i-svobodu.html

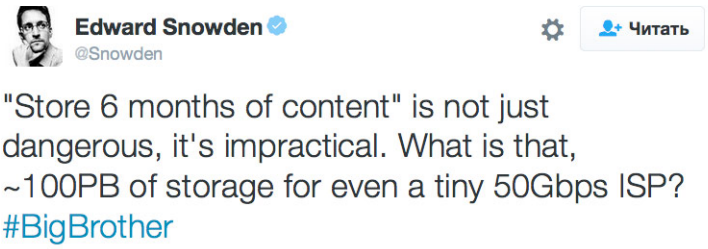

Figure 2. Edward Snowden's critical tweet on the duration of data storage outlined in the Yarovaya law.

While SORM and Yarovaya law give FSB access to data stored on Russian servers without informing site owners or providers, it is more difficult to get access to foreign services, e.g. Facebook and Twitter. Thus, a set of new measures has been adopted to reconfigure data storage and transfer.

2.2. "Snowden Effect" on RuNet: Migrations of Personal Data

Snowden's revelations had a considerable effect on IT markets. The leaks "changed the way people perceive their personal data, and will cost internet corporations, especially American ones, millions of dollars" (Filonov, 2014). Indeed, in January 2014, Canadian provider Peer1 showed that 75 British and Canadian companies did not want to store their data in the US because of the fear of being tracked down by the surveillance services.[13] Internet companies started creating servers outside US territory.

Russian Internet users—particularly specific groups including developers and activists—were seemingly not caught unprepared by Snowden's revelations. SORM being well-known since the late 1990s to all active Internet users, it was not news for Russians that governments could track their communications without a court order. Maxim I., hosting provider with Komtet, notes: "His revelations were not a surprise for specialists….In Russia, and I am sure, in any country, it is possible to get whatever information about a user or his websites. Some RuNet users even joked about the role Snowden played in RuNet regulation: 'Why have they kept Snowden here?' Very simple. They just asked him about the downsides of the American system of surveillance and made a better one".[14]

Snowden's revelations attracted attention to existing surveillance practices and made it possible to compare SORM with the US system. However, the revelations' most important impact concerned the role of US cloud services and internet corporations. In response, the Russian government modified the "Law on storage and protection of personal data" and reconsidered data geopolitics to allegedly guarantee the "protection of Russian citizens' data from US government surveillance". Researcher-journalists Andrei Soldatov and Irina Borogan insist on the role that Snowden played in this: "Right on time, Edward Snowden appeared on the world stage. The NSA scandal made a perfect excuse for Russian authorities to launch a campaign to bring global web platforms such as Gmail and Facebook under Russian law—either requiring them to be accessible in Russia by the domain extension .ru, or obliging them to be hosted on Russian territory" (Borogan & Soldatov, 2013).

The law #242-FZ was adopted on 1 September 2014. It obliges providers to "store personal data of Russian citizens, used by internet services, on the territory of the Russian Federation". Providers must guarantee recording, systematization, accumulation, storage, updates, modifications and extraction of personal data using databases located on Russian territory.[15] Non-compliance with this new law may result in total blockage of the service. Thus, for example, in November 2016 LinkedIn was blocked in Russia (including mobile apps) for the violation of the new data storage policies. Web services are also required to build backdoors for Russian secret services to access stored data. Another way to put pressure on western companies is to block entire web services because they store "forbidden information". Thus, YouTube was blocked in Russia for hosting a video judged as extremist. Facebook removed a page called Club Suicide rather than seeing its entire network blacklisted. The repatriation of data illustrates the tendency of Russian internet governance towards "digital sovereignty" (Nocetti, 2015, p. 112).

Several resistance tactics have developed in response to these balkanization measures. A petition addressed to Google, Facebook and Twitter asks them not to oblige: "We don't trust the domestic security services that are in charge of data security once the data is in Russia. We're asking internet companies to withstand this pressure using all possible legal means and we are ready to support them".[16] Developers were immediately concerned, as the law attacked the instruments they were constantly using, such as GitHub, as well as their data storage practices. Another tactic deployed was a reorientation towards new products that would avoid storage of personal

[13] Available at http://go.peer1.com/rs/peer1/images/Peer1-Report-NSA-Survey-NA.pdf
[14] Available at http://www.yaplakal.com/forum1/st/75/topic1086610.html
[15] Available at http://www.garant.ru/news/648095/#ixzz4LqmT7iT8
[16] Available at https://www.change.org/p/facebook-google-twitter-don-t-move-personal-data-to-russia

data: "We try to make services that do not store user data, so that we do not have to store it on our servers", remarks Alexey P., developer, CTO of Progress Engine; "We have some apps that we make for TV, or for electronic wallets, where the data is stored on the servers of our clients". These are specific resistance tactics which we could call tactics of "evasion". In fact, instead of contesting the law #242-FZ by communicating directly with the Russian government, citizens either try to communicate with western IT companies (addressing petitions to Google and Facebook), or modify their own practices and professional activities in order to find legal gaps or grey zones (e.g. using APIs for authorization or third parties for user data storage, or repositioning their product in order to use no personal data at all).

Another step towards digital sovereignty was made in spring 2016 with an ambitious project of "state-in-the-middle": during the forum "IT + Sovereignty", the intended creation of state-owned SSL-certification was announced. Forum member Natalya Kasperskaya explains: "Roskomnadzor and FSB are lobbying the delegation of SSL certificates to governmental organizations….Now we have a piece of the Internet that is completely out of control by our own country, and it is not good. Because the data is being gathered globally, by someone who is beyond the borders of our state, and it is totally wrong".[17] According to our interviewees, this project is actually a response to the inefficient Yarovaya law and the growing popularity of encryption among RuNet users. Alexey P. emphasizes: "They understood that storing gigabytes of data will give no results, especially because it is encrypted….So the project to build a Man-in-the-middle attack on the governmental level is scary".

2.3. Error 451: Filtering Websites, Restricting Access to the Content

```
HTTP/1.1 451 Unavailable For Legal Reasons

    <h1>Unavailable For Legal Reasons</h1>
  <p>This request may not be serviced in the
Roman Province of Judea due to the Lex Julia
     Majestatis, which disallows access to
   resources hosted on servers deemed to be
operated by the People's Front of Judea.</p>
                                    </body>
                                  </html>
```
[18]

A third set of measures, based on filtering, seeks to control user access to the content of websites judged as extremist or criminal. Since 2007, regional prosecutors have implemented court decisions requiring ISPs to block access to banned sites accused of extremism, but this has not been done systematically. In order to centralize these different materials, a "Single register of Internet resources containing information whose distribution is forbidden in Russia" was created in 2012: any websites that enter this blacklist have to be blocked and three governmental agencies participate in the constitution of this blacklist. Since the adoption of the "Lugovoy law" on 1 February 2014, the list includes websites that "appeal to extremism", e.g. mass disorders, religious or interethnic discord, participation in terrorist attacks or some types of public mass events.

On 13 March 2014, Roskomnadzor blocked access to four webpages: Grani.ru (a liberal online media platform), Kasparov.ru (the website of Garry Kasparov, chess-player and a leader of the liberal opposition), Ezhednevniy Zhurnal (liberal media platform) and the blog of Alexey Navalny (anti-Putin movement leader in 2011–2012 and reputable blogger). Roskomnadzor stated that "these websites contain appeals to illegal activities and participation in mass demonstrations that violate the law".[19]

The list of forbidden webpages is accessible online.[20] As of 30 September 2016, 41,064 pages—mostly concerning prostitution, gambling, black markets, gaming and torrents—are blocked. However, NGO websites are also present, such as the site of Mirotvorets,[21] a pro-Ukrainian organization that informs about the conflict in Ukraine, in particular on the location of Russian troops.

The blocking happens in three ways: by DNS, by IP address or by URL, using Deep Packet Inspection. Administratively, hosting providers are responsible for keeping the blacklist up-to-date and communicating with the owners of forbidden sites and end-users. Maxim I. notes that "The blocking is very easy. We receive and update regularly the black list, twice in a day, and we block those of our clients who are not lucky….We inform our client that his site has been added to the blacklist. Then we listen to everything that the client wants to say about Roskomnadzor but we can't help them or ignore the demand of Roskomnadzor because in this case they can block the IP address of the server, or even an address pool. I am not even speaking about administrative consequences for the company".

While providers have very little possibility to resist the blocking of the blacklisted resources, they choose other forms of action to express their critique of Internet censorship. Vladimir K., director of the ISP CLN, says: "When users try to access to a blocked page, we show them the error message that starts with a phrase: "The struggle against evil is almost never a struggle for good". Thus, the error message itself becomes a space of expression where providers can symbolically communicate with their users by showing their attitude towards the Lugovoy law.

However, Russian filtering and blocking systems are applied unevenly from one region to another, from one

[17] Available at https://rublacklist.net/21509
[18] Available at https://tools.ietf.org/html/rfc7725
[19] Available at http://www.newsru.com/russia/13mar2014/block.html
[20] Available at https://reestr.rublacklist.net
[21] Available at www.myrotvorets.center

provider to another. For example, several employees of ISPs of big companies/monopolists, such as Russian Railways, confirm that they have not been blocked, as Dmitry M. in 2014: "We have this provider in our company, and all the blacklisted websites can be opened. However this seems quite logical, because Roskomnadzor can't give any orders to Russian Railways, who own this provider" (Nossik, 2014). Also, filtering works only partially, depending on the region, the provider and its position on the market, its connections with western providers (e.g. providers who had a peering agreement with Stockholm could access blacklisted websites).

The paradox of filtering consists in the double digital divide that it creates. The more "politicized" users, familiar with the forbidden online resources, will keep on accessing them, using specific tools to bypass censorship. However, the majority of the population will be unable to access this content, lacking the necessary knowledge, resources and technologies to do so. Search engines are also impacted by filtering, so reinforcing the divide: before the blockage, users could accidentally discover some websites (e.g. Navalny's blog) through search engines, but after the blockage these sites "disappeared" (were dereferenced) from the search results. This consequently reduces considerably any potential audience and reinforces the echo-chamber effect by regrouping users who already agree, as mentioned by user popados: "These blockages are not for those who read and will bypass no matter how. It is for random visitors that come from the search or other casual channels that actually constitute the majority. They will just go to another website. In this sense, the blockage is rather efficient" (Nossik, 2014). The same phenomenon touches blacklisted torrent websites, such as Rutracker, that demonstrate a significant decrease in traffic: "the majority of users are just lazy, they are finding new open sources of content. So the goal of the filtering is not to close for everyone, but for an important part", says Maxim I.

Still, access restrictions are not especially difficult to bypass. The IETF notes that "in many cases clients can still access the denied resource by using technical countermeasures such as a VPN or the Tor network" (RFC 7725). Indeed, users deploy manifold technical practices, bricolages and *arts de faire*.

3. Elusive Users: Countermeasures for Bypass and Anonymity

> "Long ago, when GSM connection was not very high quality, there was a trick: you just need to say 'bomb, president, terrorism' and the connection would become much better" Fedor, ISP

Users recently gathered in associations to denounce RuNet censorship and surveillance and promote countermeasures: these include but are not limited to the Russian Pirate Party, *Roskomsvoboda* (Association for the Freedom of Communications), a website for monitoring and analytics of the blockages (Rublacklist), and the project Openrunet promoting countermeasures. While some of these are focused on political campaigning against access restrictions, others concentrate on promoting countermeasures and do not focus on the government but on RuNet users.

Different resistance tactics circulate on forums, blogging platforms and social networks, in the form of comments, posts or specific tutorials. Dedicated "offline" workshops, called "cryptoparties", are organized to present privacy-enhancing tools, and draw from an international cryptoparty movement launched in 2012. Pre-Snowden, in 2012, we participated in such workshops in Saint-Petersburg. They were aimed at left activists (anarchists and antifascists). After 2013, seminars were aimed at a wider audience including NGO workers, journalists, rights defenders and RuNet users seeking to adapt their habits to new realities. The event name was also adapted, the marked word "cryptoparty" being replaced by "seminars on information security".

A wide range of bypass and anonymization tactics and tools exist, circulating both on the Web and during thematic seminars. The organizers themselves attempt to classify existing tools and practices, to build tutorials and construct a coherent presentation, for which several strategies have been observed. Classification occurred, for example, based on the question "Who is your enemy?" Thus Igor, moderator of a cryptoparty for an audience of NGO workers in April 2016, Saint-Petersburg, constructed his presentation around two "big enemies": the state and corporations. He presented the tools that can help bypass state censorship and some devices that would help resist targeted advertising and data tracking. A different format was observed in the *Roskomsvoboda* tutorials, which organize materials according to the tasks users want to perform: "access to a blocked website", "communicate in privacy", "protect your metadata while surfing the web".

On our end, we distinguish such practices here according to the laws they intend to challenge, whether it is SORM or filtering practices and access to blacklisted content. Some of the tools are used in both cases.

As SORM is aimed at intercepting communications, bypassing techniques consist in encrypting them. Encryption tools are used at both the application and network layers. At the application layer, cryptography has been promoted since the first campaigns against SORM launched in 1998 by Moscovskiy Libertarium.[22] Back then, activists were promoting PGP or GnuPG over a mail client, all the while understanding the limits of cryptography: "These countermeasures can't *exclude* the possibility to intercept your communications, but our goal is to make this access extremely hard and *expensive*" (Otstavnov, 1998, our emphasis). Moskovskiy Libertarium was promoting massive usage of these tools

[22] Available at http://www.libertarium.ru/sorm_crypto_esc

as collective action to make surveillance hard and economically disadvantageous for the state: "If the Internet community used these technical means at least in half of the cases, it would become almost immunized against all these dirty tricks such as SORM. However, even occasional usage of strong crypto (especially for fun) will make our opponents' work very hard" (Otstavnov, 1998).

Nowadays, usage of PGP has increased, while remaining far from the ambitious goal of 50% or 100% of users; however, mobile apps for encrypted messaging are gaining popularity. The market for encrypted messaging and mailing clients being in expansion (Ermoshina, Musiani, & Halpin, 2016), cryptoparty organizers and specialized NGOs (e.g. Roskomsvoboda) elaborate several sets of criteria to rate and compare the apps. For example, Igor, the moderator mentioned above, presented a set of criteria including open source, end-to-end, group chat and calls, synchronization between devices, self-destroying messages, notifications about logins from different devices, logging history and multi-layered authentication.

For the time being, alongside WhatsApp,[23] Telegram remains the most popular secure messaging app among Russian users. The usage of Telegram varies according to users' goals and threat models. Several functionalities of the app make it convenient for different user groups: chats, secret chats, group chats, bots and channel broadcasting. Users faced with a low level of threat, not associated with any political activities, tend to adopt Telegram as an alternative to WhatsApp and SMS for everyday conversations with their peer groups. Many activists and privacy-concerned users are aware of the absence of "privacy by default" in Telegram chats (client-to-server encryption) and opt for a "secret chat" option that offers end-to-end encryption. This user group also adopts two-step authentication and self-destruct timer options. Functions such as "Group chat" are used for group conversations between up to 200 users and are popular among activists, journalists or researchers for organizational purposes, as an alternative to Google Groups or mailing lists. For example, one of our use-cases, a group of researchers working in Eastern Ukraine, use Telegram on a daily basis to coordinate research activities, discuss fieldwork, materials and other organizational information. However, they do not rely on Telegram for very sensitive discussions and prefer face-to-face offline meetings.

The popularity of Telegram in Russia can be partly explained by the reputation of its founders, Nicolai and Pavel Durov, Russian-born developers and entrepreneurs. Pavel Durov, the founder of Vkontakte, the most famous Russian social network, is colloquially referred to as the "Russian Zuckerberg" and became *persona non grata* in Russia after his refusal to collaborate with the FSB.[24] Telegram's quick rise on the market of messaging apps is of particular interest as it tells us a lot about the socio-economic factors that influence the success of an innovation in the field: it was when Facebook bought WhatsApp (followed by a several hours blackout for the latter), that the Telegram download rate exploded. As opposed to WhatsApp, Telegram can publicly underline its non-for-profit character and lack of ties with any commercial or governmental services.

While the Russian version of Telegram was released in 2012, before the Snowden revelations, Durov claims that the international version of his tool was inspired by the whistleblower: "In 2012 my brother and I built an encrypted messaging app for our personal use—we wanted to be able to securely pass on information to each other, in an environment where WhatsApp and other tools were easily monitored by the authorities. After Edward Snowden's revelations in 2013 we understood the problem was not unique to our situation and existed in other countries. So we released the encrypted messaging app for the general public".[25]

As Telegram servers are located in five different countries around the world, outside Russia, its broadcasting function is used by censored media as a way to bypass the blockage, and by bloggers as an alternative to Facebook and traditional blogging platforms (for example, Alexey Navalny's popular bot on Telegram and the Grani.ru channel and bot, amongst others). However, unlike private communications on Telegram, public channels may be read and blocked by ISPs and by the Telegram technical team. As of January 2016, 660 channels attributed to ISIS were blocked.

While the "broadcasting channel" function made Telegram an alternative to other news sources and social networks, political activists prefer either the "secret chat" function, or Signal. The Signal application, which Snowden recommended, is used for a specific and limited set of functions—SMS and phonecalls. However, at recent cryptoparties Signal has been criticized for the absence of functions such as automatic synchronization among different devices, time-settings and search.

The technologies used to bypass the Lugovoy law and access censored websites mostly employ the practice of IP address-switching. Therefore one of the most popular and easy-to-use tools is an online proxy server,such as hideme.ru or cameleo.ru. However, this system was criticized by our IT-security activist interviewees for its lack of traffic encryption: a proxy is only useful for by-

[23] We do not examine WhatsApp here, as it was not initially designed as a secure messaging app with end-to-end encryption. Our research and interviews with developers of secure messaging apps (especially with Peter Sunde from Heml.is, who had been contacted by WhatsApp before they decided to purchase the Signal protocol) also show that WhatsApp's motivation to adopt encryption was a market-driven choice, not an ideological decision. Even though the consequences of WhatsApp's decision are very important for the overall "passive" adoption of encryption in Russia, what interests us in this paper is the deliberate and intentional choice of a secure tool. We also do not have data measuring the explicit adoption of WhatsApp consequent of its turn to end-to-end encryption.

[24] Available at http://www.reuters.com/article/idUS74722569420130830

[25] http://www.dazeddigital.com/artsandculture/article/24279/1/pavel-durov

passing the blockage to access content from a blacklisted website, but it does not hide the content that a user is reading. Users are also creatively adapting existing tools to achieve the bypassing goal. For instance, Russians actively use Net archives (archives.org, archive.is or cached versions of websites stored by Google), or activate the "turbo" mode in Opera or Yandex browsers, enabling a very high speed of data transfer. However, once again these tools merely give access to the blocked page, but do not guarantee any anonymity. Moreover, in November 2016, Roskomnadzor started negotiations with Opera representatives about the possibility of blocking access to forbidden content even in "turbo" mode. As of January 2017 no agreement has yet been reached, due to Opera having recently been sold to Golden Brick Capital, a Chinese investment consortium.

As users can be tracked and eventually persecuted for their search of forbidden materials, a set of anonymizing network-layer tools is promoted through cryptoparties and online tutorials, starting with Tor. However, this popular tool is increasingly criticized. Snowden's revelations proved the importance of metadata protection and exposed the vulnerability of Tor. While seminars on informational security observed before 2013 in Saint-Petersburg were promoting widespread use of Tor with almost no attendant criticisms, more recent observations (2015 and 2016) show a growing skepticism and loss of trust. Igor explained the vulnerability of Tor at a workshop organized by Teplitsa Sotsialnih Technologiy: "First of all, your internet service provider will see that you use Tor. That gives him, and the people behind him, a reason to be attentive to you: who is this person who is constantly using Tor? Snowden said that the NSA is tracking everybody who uses Tor, automatically. There are only 7,000 exit nodes in the Tor network, it is not that complicated to track them all".

Another type of network layer tools is a Virtual Private Network (VPN), which adds a supplementary layer of traffic protection. Some of our interviewees pointed out that VPN usage "has become a norm" for them after the GitHub blocking incident in Russia. Among the trusted VPN plugins, activists prefer "zenmate"[26] and "tunnelbear",[27] as they do not need to access user data, while other apps demand the right to access the memory card, photos and contacts. Another popular VPN is offered by Riseup.net,[28] which has a good reputation among politically engaged users ("done by activists for activists"). However, along the lines of Ethan Zuckerman's "cute cat theory of digital activism" (2008), users point out that activist-oriented tools are more vulnerable to targeted attacks than are general public-oriented tools.

Snowden's revelations had a pedagogical effect on Russian activist communities: during observed cryptoparties they were repeatedly heard to emphasize the global character of the surveillance phenomenon. Information security advocates insisted on the necessity for users to change their whole "lifestyle", including interaction with different devices and publishing on social networks. Igor remarks: "You can encrypt your traffic as you wish, you can hide, but if you go to Vkontakte and publish your photo, or talk about revolution, you must understand that it is extremely easy to de-anonymize you and track your network of friends. So start by using your brains, before using Tor and VPN". Thus, after Snowden revealed the interests of big corporations in collecting user-generated data, cryptoparties began to focus not only on activist use cases but on everyday life habits, "unboxing" mobile devices and laptops to demonstrate customization of privacy settings.

On their end, activists are learning how to program message self-destruction or deactivate the tracking of search history and location. Encryption of mobile devices and usage of pass-paragraphs and double or triple authentication methods (combining fingerprints, password and a figure) are becoming popular alongside the use of anonymous search engines such as StartPage or DuckDuckGo, adblocking plugins and cookie controls. Activists advocate multilayered protection and encryption by combining virtual machines, VPN, TOR and encrypted mail and messaging clients.

Finally, Snowden's revelations on NSA surveillance enabled a comparison of the Russian SORM and US intelligence strategies, showing common points and important differences between the two surveillance systems. Activists describe the Russian system as less efficient than its US counterpart, pointing to the geopolitical reasons behind this gap. Not only is Russian surveillance less effective, but the diplomatic context and IT-market configuration also make it harder for Russian surveillance services to be as omnipresent as US ones. Yuriy, an activist, developer and participant in the April 2016 workshop, notes: "As we now know from Edward Snowden's leaks, Americans have their own kind of SORM deployed by the NSA. But it is much more expanded than SORM, it has lots of subdivisions, some of them really crack servers, some others do cryptoanalytics. Snowden claims American services have managed to somehow survey even the Tor traffic, by taking control over the exit nodes. But well…I am really not sure whether it is possible for Russian services to control exit nodes, because sometimes they are located, I don't know, in Panama. And the NSA has much more power to control exit nodes in different countries than Russia. No one likes Russia, and Russia likes no one. It is much more complicated for the FSB to negotiate the access". Therefore it is the controversial position of Russia within the international political arena that makes it harder to negotiate with Western companies to control the traffic of Russian citizens who use anonymizers and Tor.

[26] Available at https://zenmate.com
[27] Available at https://www.tunnelbear.com
[28] Available at https://riseup.net/en/vpn

4. Migrating Servers (and People): A Geopolitical Countermeasure

Due to this geopolitical aspect of RuNet governance, another effective protection tactic is the physical migration of servers and people. Indeed, the legal and technical constraints of RuNet result not only in individual strategies for bypassing and collective action and campaigning, but also in a significant exodus of Web professionals, especially journalists of online media.

The emigration of Russian journalists is not new. In the USSR a significant number of journalists left the country as a result of political persecution (De Tinguy, 2004). However, in the 2010s these exiles are paradoxical, because even if they leave the country they remain connected to Russian cyberspace and actively contribute to its development (Bronnikova, 2016).

Media websites Grani.ru and Meduza were shut down by Roskomnadzor in 2014, making it extremely hard for their editors and owners to survive economically. Despite bypassing tools, their audience decreased. This resulted in the migration of infrastructure and of some journalists out of the Russian Federation. Yuliya Berezovskaya, from Grani.ru, left for France, while Meduza was dislocated to Riga. The cases of Grani.ru and Meduza are interesting for reconsidering the notion of "brain drain". Indeed, the Internet connects migrant and non-migrant populations in their transnational online engagement (Diminescu, 2008; Nedelcu, 2010): online journalists and bloggers expatriated in the European Union, the US or Israel are not excluded from Russian political life but remain important actors in the RuNet freedom quest. For example, Meduza actively informs its readers about recent updates in Russian Internet governance.

Such expatriation also takes shape in a diaspora of infrastructures. In particular, what are called "mirrors" of forbidden websites are created, using platforms such as Amazon.[29] An increasing number of NGOs and other associations opt to transfer their hosting to outside of Russia. As Maxim I., a hosting provider, observes: "Such websites as Children 404[30] or oppositional websites are progressively transferred to foreign servers and start using non-Russian gTLDs (generic top-level domains, such as .ORG). The reason for this is simple: without any court decision your page or the entire website can be blocked, sometimes even by mistake, as it happened with Google or GitHub. I remember also a mass exodus of clients in Belarus, after they have been obliged to work only in Byelorussian data-centers". The tactic of domain zone migration was also adopted by Grani.ru which moved to the .org domain zone on 27 May 2016, two years after its chief editor physically left Russia. Another tactic of "exodus" concerns the kinds of platforms used to disseminate content: more and more of Russia's liberal online media are abandoning the traditional format of websites or blogs in favor of social media pages or Telegram broadcasting channels.

Interestingly, this exodus had begun even before the "Law on Personal Data Storage": Alexey Sidorenko, director of the NGO *Teplitsa Sotsialnih Technologiy*,[31] dates the first wave of infrastructure migration back to 2010. The second wave of digital migration can be attributed to the "Foreign Agent" law: Teplitsa itself had to move from Moscow to Warsaw after the clampdown on foreign aid agencies. IT specialists have seldom been using Russian data-centers because of their technical drawbacks: "People have been actively using western platforms, just because it is more useful and efficient", says Russian-born, Turkey-adopted developer Timofey. However, recent regulation of the Internet has modified the practices of developers and reconfigured the markets. Alexey, CTO of Progress Engine, concludes: "If GitHub is closed, this will enforce brain-drain. And it has already started, several of my colleagues have left to Germany. Folks prefer to work with foreign markets and foreign services. First of all, it's the quality of technological solutions. And also, when you work with a western client, there's a possibility to move. If there's more control from the government, you have a chance to leave".

5. Conclusions

As Edward Snowden is currently on (temporary) asylum in Russia, numerous scholars and journalists insist on the geopolitical significance of this act and emphasize its importance within the global context of a "Cold War 2.0". Yet, far from supporting Snowden's fight for transparency of government data and Internet users' freedom, the Russian government is gradually centralizing its surveillance over the RuNet. However, the direct and indirect influence of the Snowden revelations is making itself visible in a number of other ways, by exposing censorship and surveillance at an unprecedented scale and encouraging creative responses to it. This article has explored how, in response to growing censorship, a variety of tactics are being developed and deployed by Russian users and content producers, ranging from infrastructure-based countermeasures and *détournements* to geopolitical reconfigurations involving the migration of hardware and people.

Although it is not within the scope of this paper to estimate the long-term impact of recent mobilizations (as we do not have enough data to measure this), we can conclude that Russian civic mobilization may be analyzed at two levels. The first is public and collective, for example the "anti-SORM" movement or petitions against Yarovaya law. Such movements appear to have limited impact beyond encouraging visibility and draw-

[29] *Reporters without Borders*, having experimented this technique with Chinese bloggers, helped Russian blacklisted media to put it in practice. Thus, mobilizations for RuNet freedom are integrated in transnational campaigns.

[30] NGO defending the rights of LGBTQI-children.

[31] Teplitsa Sotsialnih Technologiy is an NGO specialized in IT-education of social workers and activists and in development of collaboration between Russian non-profit organizations and IT-specialists. Available at https://te-st.ru

ing public attention to the problem, and even so they remain limited to a small section of the population (with only around 600,000 signatures on Change.org and 2,000 people in attendance at the anti-Yarovaya law meeting), namely IT professionals, journalists, bloggers and Internet freedom activists. However, at the second level, that of so-called "evasion" tactics, mobilisation is far more successful: far from being a contentious means to criticize government or affect changes in legislation and Internet policy, these invisible or elusive techniques have a direct and immediate impact on the everyday practices of users and IT professionals. Evasion techniques are based on an ingenious and constantly changing set of tools and *arts de faire*, and can help to access or broadcast forbidden content as well as to continue IT-related business.

This article shows that Russian Internet governance increasingly takes shape as an "infrastructural battle", a dialectic between the government, who use and co-opt infrastructure, and users, developers and providers who hijack and reconfigure it, in a constant co-shaping of law and technology. This speaks to the "turn to infrastructure" we have recently explored as an increasing tendency in Internet governance (Musiani, Cogburn, DeNardis, & Levinson, 2016). If the Snowden revelations have constituted the 'perfect excuse' for the Russian government to try to enforce a radical approach of "digital sovereignty" (Nocetti, 2015), they have also become on the one hand a catalyst of freedom activists' mobilization, not only for "power users" but for the everyday situated practices of lambda users, and on the other hand an opportunity for Russian businesses working with Western companies to fight both from within and from outside the country. Moreover, the specific geopolitical and economic conditions of embargo can be understood as an important obstacle for Roskomnadzor. It is not civil society but rather Russia's lack of resources, infrastructure, expertise and technologies that make it impossible, at least for now, to apply this law in practice. Despite the current escalation of surveillance, could Russia's controversial position on the international chessboard turn into a paradoxical opportunity for the RuNet?

Acknowledgements

This work is supported by the European Union's Horizon 2020 Framework Programme for Research and Innovation (H2020-ICT-2015, ICT-10-2015) under grant agreement nº 688722—NEXTLEAP.

Conflict of Interests

The authors declare no conflict of interests.

References

Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation, *Education Permanente*, *134*, 78–89.

Borogan, I., & Soldatov, A. (2013). Russian surveillance state. *World Policy*. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Bronnikova, O. (2016). Publikovat dlya Rossii iz-za granitsi. Internet—prostranstvo bez granits? [Publishing for Russia from abroad. Is internet a borderless space?]. In F. Daucé, B., Ostromooukhova, O., Bronnikova, & A. Zaytseva (Eds.), *Nezavisimye ot kogo? Alternativnye SMI, malye izdatelstva i bloggery v sovremennoy Rossii [Independent from whom? Alternative mass-media, small editors and bloggers in contemporary Russia]*. Moscow: NLO. Book in preparation.

Ceruzzi, P. (2006). The materiality of the Internet. *IEEE Annals of the History of Computing*, *28*(3), 96–97.

De Tinguy, A. (2004). *La Russie et les Russes depuis l'ouverture du rideau de fer*. Paris: Plon.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. Cogburn, L. DeNardis, & N. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 3–21) New York, NY: Palgrave-Macmillan.

Diminescu, D. (2008). The connected migrant: An epistemological manifesto. *Social Science Information*, *47*(4), 565–579.

Elting, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J., & Gasser, U. (2010). *Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization* (Report no. 2010–11, October 19, 2010). Cambridge, MA: Berkman Center for Internet and Society.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-end encrypted messaging protocols: An overview. *Proceedings of Internet Science Conference 2016* (pp. 244–254). Florence, Italy: University of Florence.

Erpyleva, S., & Magun, A. (Eds.). (2014). *Politika Apolitchnyh: Grazhdanskie Dvizheniya V Rossii 2011–2013 Godov. [Politics of apolitical: Civic movements in Russia in 2011–2013]*. Moscow: Novoe Literaturnoye Obozrenie.

Filonov, D. (2014, August 12). Otlozhennyi effekt. Kak Snowden zastavil Acronis potratitsya na servery [Postponed effect. How Snowden made Acronis spend money for the servers]. *Forbes.ru*. Retrieved from http://www.forbes.ru/tekhnologii/tekhnika-i-biznes/265017-otlozhennyi-effekt-kak-snouden-zastavil-acronis-potratitsya-na

Freiberg, P. (2014). *Putin's Russia—On a path to cyber sovereignty?* Retrieved from http://www.academia.edu/10762446/Future_of_Internet_Freedom_in_Russia

Gelman, V. (2010, March 9). Lovushka polusvobody: The trap of a half-freedom. *Slon.ru*. Retrieved from http://slon.ru/russia/lovushka_polusvobody-310531.xhtml

Kantyshev, P. (2016, September 4). Rostehu Nuzhno 10,3 Milliarda Rubley na Razrabotky Paketa Yarovoj [Rostech needs 10.3 mlrds of Rubles to develop Yarovaya Law]. *Vedemosti*. Retrieved from http://www.

vedomosti.ru/technology/articles/2016/09/05/655653-rostehu-zakona-yarovoi

Kharkhordin, O. (2011). *Ot obshchestvennogo k publichnomu: kollektivnaia monografiia [From social to public: Collective monograph]*. Berlin: EUSP Press.

Klyueva, A. (2016). Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society. *International Journal of Communication*, *10*, 4661–4680.

Kozlov, V., & Filipenok, A. (2016, August 9). Miting protiv zakona Yarovoy v Moskve sobral neskolko tysyach chelovek [Meeting against Yarovaya law gathered several thousand people]. *RBC*. Retrieved from http://www.rbc.ru/politics/09/08/2016/57aa0a259a79470ed51332fd

Latour, B. (1988). *The pasteurization of France*. Cambridge, MA: Harvard University Press.

Lonkila, M. (2012). *Russian protest on- and offline. The role of social media in the Moscow opposition demonstrations in December 2011* (FIIA Briefing Paper 98). Helsinki: The Finnish Institute of International Affairs.

Musiani, F., Cogburn, D., DeNardis, L., & Levinson, N. (Eds.). (2016). *The turn to infrastructure in internet governance*. New York, NY: Palgrave-Macmillan.

Nedelcu, M. (2009). Du brain drain à l'e-diaspora: Vers une nouvelle culture du lien à l'ère du numérique? *TIC et Sociétés*, *3*(1). Retrieved from http://ticetsociete.revues.org/675

Nocetti, J. (2015). Russia's "dictatorship-of-the-law" approach to internet policy. *Internet Policy Review*, *4*(4). doi:10.14763/2015.4.380

Nossik, A. (2014, March 19). *Dyryavoe sito censury [Leaky strainer of censorship]*. Retrieved from http://dolboeb.livejournal.com/2652283.html

Otstavnov, M. (1998, June 26). *Chifrovaniye I SORM—Tchastnoye mnenie [Encryption and SORM"—A personal opinion]*. Retrieved from http://www.libertarium.ru/l_sorm_cryptsorm

Prozorov, S. (2012). Vtoroj konec istorii: Politika bezdejatelnosti ot perestrojki do Putina [The second end of History: The politics of inactivity from Perestroika to Putin]. *Neprikosnovennyj zapas*, *2*(82), 169–191.

Schepin, A. (2016, August 1). Irkutskie Operatory Svyazi O Nedostatkah Paketa Yarovoy [ISPs from Irkutsk: On the drawbacks of Yarovaya Package]. *IRK*. Retrieved from https://www.irk.ru/news/articles/20160801/package

Volkov, L. (2016, March 24). *Pedofil Na Slujbe FSB: Kto Sledit Za Nami v Internete? [A pedophile that serves FSB: Who is surveilling us in the internet?"]*. Retrieved from https://www.leonidvolkov.ru/p/119

Zhuravlev, O., Savelyeva, N., & Yerpylova, S. (2014). Individualizm I solidarnost v Novyh Rossijskyh Grazhdanskih Dvizheniyah [Individualism and solidarity in new Russian civic movements]. *Journal of Social Policy Studies*, *12*(2), 185–200.

Zuckerman, E. (2008, March 8). *The cute cat theory talk at ETech*. Retrieved from http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech

About the Authors

Ksenia Ermoshina (PhD, MINES ParisTech, 2016) is a postdoctoral researcher at the French National Centre for Scientific Research (CNRS), Institute for Communication Sciences (ISCC-CNRS/Paris-Sorbonne/UPMC). Ksenia is working with the European H2020 project NEXTLEAP (2016–2018, Next-Generation Techno-Social and Legal Encryption, Access and Privacy). She is also co-chair of Emerging Scholars Network of the International Association of Media and Communication Research.

Francesca Musiani (PhD, MINES ParisTech, 2012) is Associate Research Professor (*chargée de recherche*), French National Centre for Scientific Research (CNRS), Institute for Communication Sciences (ISCC-CNRS/Paris-Sorbonne/UPMC), associated researcher with the Centre for the Sociology of Innovation of MINES ParisTech-PSL, and academic editor for the *Internet Policy Review*. She is currently one of the Principal Investigators for the European H2020 project NEXTLEAP (2016–2018, Next-Generation Techno-Social and Legal Encryption, Access and Privacy).